UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

Anita McMillon, *on behalf of herself and all others similarly situated,* Plaintiff, v. Illinois Gastroenterology Group, P.L.L.C., (d/b/a "Illinois Gastroenterology Group"), Defendant.	Case No. _____ Hon. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Anita McMillon ("Plaintiff) brings this Class Action Complaint against Illinois Gastroenterology Group, P.L.L.C. ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including names, addresses, and Social Security numbers, driver's license, Passport, financial account information, payment card information, employer-assigned identification number, (collectively, "personally identifiable information" or "PII"), medical information ("protected health information" or "PHI"), and biometric data ("protected biometric information" or "PBI") .

2. According to Defendant's website, "[Defendant] was formed in 2010 …and is the largest single specialty GI group in Illinois, with over 40 gastroenterologists." [1]

[1] https://www.illinoisgastro.com/about (last visited Apr. 26, 2022).

3. On October 22, 2021, Defendant discovered unusual activity within its computer network. (the "Data Breach"). Defendant launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event

4. On November 18, 2021, the investigation determined that an unauthorized actor gained access to Defendant's systems and that information contained in those systems may have been viewed or taken by the unauthorized actor. [2]

5. On March 22, 2022, approximately five months after Data Breach was confirmed, Defendant "determined the personal information of individuals including the following types of information that [Defendant] maintains in its systems and that were, or may have been, impacted by this incident include: name, address, date of birth, Social Security number, driver's license, Passport, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data." [3]

6. By obtaining, collecting, using, and deriving a benefit from the PII, PHI, PBI of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII, PHI, and PBI impacted during the Data Breach included names, addresses, dates of birth, Social Security numbers, driver's license, Passport, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data.

7. The exposed PII, PHI, and PBI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII, PHI, and

[2] https://www.prnewswire.com/news-releases/illinois-gastroenterology-group-pllc-provides-notice-of-a-security-incident-301531255.html (last visited Apr. 26, 2022).
[3] *Id*.

PBI to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves.

8. This PII, PHI, and PBI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII, PHI, and PBI of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited several months to report it to government agencies and affected individuals. Indeed, as of April 26, 2022, Defendant has still not reported the breach to government agencies. Upon information and belief, Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiff and Class Members of that information.

9. As a result of this delayed response, Plaintiff and Class Members had no idea their PII, PHI, and PBI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII, PHI, and PBI was compromised as a result of Defendant's failure to: (i) adequately protect the PII, PHI, and PBI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII, PHI, and PBI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII, PHI, and PBI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud,

and/or unauthorized use of their PII, PHI, and PBI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and substantially increased risk to their PII, PHI, and PBI which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII, PHI, and PBI.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII, PHI, and PBI of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII, PHI, and PBI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Anita McMillon is a Citizen of Illinois residing in DuPage County, Illinois.

14. Defendant Illinois Gastroenterology Group, P.L.LC., is a corporation organized under the laws of Illinois, headquartered at 20 Tower Ct., Gurnee, Illinois, with its principal place of business in Gurnee, Illinois.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently

unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d). This is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

18. The Northern District of Illinois has personal jurisdiction over Defendant named in this action because Defendant and/or their parents or affiliates are headquartered in this District and Defendant conducts substantial business in Illinois and this District through its headquarters, offices, parents, and affiliates.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

20. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII, PHI, and/or PBI, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

21. Plaintiff and Class Members relied on Defendant to keep their PII, PHI, and PBI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their PII, PHI, and PBI.

22. Defendant had a duty to adopt reasonable measures to protect the PII, PHI, and PBI of Plaintiff and Class Members from involuntary disclosure to third parties.

23. Defendant's privacy notice states, "Protecting the privacy of healthcare information is a responsibility we take very seriously. We understand that healthcare information is personal and the importance of keeping it confidential. We are committed to our established practices and procedures to protect the confidential nature of your healthcare information."[4]

24. Defendant's privacy notice states, "We are required by law to maintain the privacy of your health information and provide you notice of our legal duties and privacy practices with respect to your health information. We will abide by the terms of this Notice." [5]

25. On April 22, 2022, Defendant notified PRNewswire of the Data Breach ("Notice of Data Breach"). [6] Defendant advised that the information potentially impacted in the Data Breach, included names, addresses, dates of birth, Social Security numbers, driver's licenses, Passports, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data.

26. The Notice of Data Breach stated, in relevant part, the following:

> On October 22, 2021, [Defendant] discovered unusual activity within its computer network. Defendant immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. On November 18, 2021, the investigation determined that an unauthorized actor

[4] Notice_of_Privacy_Practices-3-13_2.pdf (illinoisgastro.com) (last visited Apr. 26, 2022).
[5] *Id*.
[6] https://www.prnewswire.com/news-releases/illinois-gastroenterology-group-pllc-provides-notice-of-a-security-incident-301531255.html (last visited Apr. 26, 2022).

> gained access to certain [Defendant] systems and that information contained in those systems may have been viewed or taken by the unauthorized actor.
>
> [Defendant] reviewed the information contained within the systems to identify if any individuals' personal information or protected health information was potentially impacted. On March 20, 2022, [Defendant] determined personal information of individuals including the following types of information that [Defendant] maintains in its system and that were, or may have been, impacted by this incident include: name, address, date of birth, Social Security number, driver's licenses, Passport, financial account information, payment card information, employer-assigned identification number, medical information, and biometric data. To date, [Defendant] has not received any reports of fraudulent misuse of any information potentially impacted.
>
> [Defendant] takes this incident and the security of personal information in its care seriously. [Defendant] moved quickly to investigate and respond to this incident, assess the security of its systems, and notify potentially affected individuals. In response to this incident, [Defendant] augmented its policies and procedures addressing network security. [Defendant] accelerated the implementation of an enhanced managed Security Operations Center including the deployment of an endpoint detection and response platform in response to this event with policies enabled specifically for ransomware. [Defendant] immediately reset passwords and employees with privileged access to sensitive systems were enrolled into our multifactor authentication platform. [Defendant] is also notifying potentially affected individuals so that they may take further steps to protect their information, should they feel it is appropriate to do so.

27. Defendant admitted in the Notice of Data Breach that unauthorized third persons accessed files that contained Plaintiff's and Class's Members' PII, PHI, and PBI.

28. The unencrypted PII, PHI, and PBI of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII. PHI, and PBI may fall into the hands of companies that will use the detailed PII, PHI, and PBI for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII, PHI, and PBI of Plaintiff and Class Members.

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, PHI, and PBI.

30. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[7]

31. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

[7] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[8]

32. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up

[8] *Id.* at 3-4.

for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[9]

33. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

[9] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[10]

34. Given that Defendant was storing the PII, PHI, and PBI of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

35. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII, PHI, and PBI of Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores the PII, PHI, and PBI of Plaintiff and Class Members.

36. Defendant acquired, collected, and stored the PII, PHI, and PBI of Plaintiff and Class Members.

37. By obtaining, collecting, and storing the PII, PHI, and PBI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII, PHI, and PBI from disclosure.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, PHI, and PBI and relied on Defendant to keep their PII, PHI, and PBI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII, PHI, and PBI and Preventing Breaches

[10] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

39. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII, PHI, and PBI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a decade or more.

40. Defendant's negligence in safeguarding the PII, PHI, and PBI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

41. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII, PHI, and PBI of Plaintiff and Class Members from being compromised.

42. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

43. The ramifications of Defendant's failure to keep secure the PII, PHI, and PBI of Plaintiff and Class Members are long lasting and severe. Once PII, PHI, and PBI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

[11] 17 C.F.R. § 248.201 (2013).

[12] *Id*.

Defendant negligently, recklessly, and intentionally disclosed and failed to protect Plaintiff's and Class Members' PBI

44. In the early 2000's, major national corporations started using Chicago and other locations in Illinois to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing, yet unregulated technology. *See* 740 ILCS 14/5.

45. In late 2007, a biometrics company called Pay By Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which are unique biometric identifiers that can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

46. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5. BIPA is an informed consent statute that achieves its goal by making it unlawful for a company to disclose information unless: "(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure

completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." ILCS 740 14/15(d)(1)-(4).

47. BIPA also states that "[a] private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers, and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." ILCS 740 14/15(d)(1)-(4).

48. As a result of the Data Breach, Defendant violated ILCS 740 14/15(d)(1)-(4) because it disclosed or disseminated Plaintiff's and Class Members' PBI without authorization or under the approved exceptions.

49. As a result of the Data Breach, Defendant violated ILCS 740 14/15(e) because it failed to protect Plaintiff's and Class Members' PBI within the industry standard and failed to protect PBI the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

50. Defendant was negligent in unlawfully disclosing and failing to protect Plaintiff's and Class Members' PBI.

51. Defendant was reckless in unlawfully disclosing and failing to protect Plaintiff's and Class Members' PBI.

52. Defendant was intentional in unlawfully disclosing and failing to protect Plaintiff's and Class Member's PBI.

53. As a direct result of the Data Breach, Plaintiff and Class Members have suffered substantial harm due to the unlawful disclosure of their PBI.

54. As a direct of the Data Breach, Defendant has harmed Plaintiff and Class Members by failing to protect PBI from unauthorized third parties.

Value of PII, PHI, and PBI

55. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

56. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Oct. 27, 2021).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Oct. 27, 2021).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 27, 2021).

> name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

57. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

58. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

---

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 27, 2021).

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Oct. 27, 2021).

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

61. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

62. The fraudulent activity resulting from the Data Breach may not come to light for years.

63. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

64. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII, PHI, and PBI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

65. According to account monitoring company LogDog, medical data, such as PHI and/or PBI, sells for $50 and up on the Dark Web.[19]

66. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

---

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 23, 2021).

[19] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

67. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII, PHI, and PBI of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

68. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII, PHI, and PBI.

69. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

70. To date, Defendant has offered Plaintiff and Class Members only 12 months of identity and credit monitoring services through Experian. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII, PHI, and PBI at issue here. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services.

---

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

71. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII, PHI, and PBI of Plaintiff and Class Members.

Plaintiff's Experiences

72. Plaintiff entrusted her PII, PHI, and PBI to Defendant.

73. Plaintiff received Defendant's Notice of Data Breach on May 5, 2022. The notice indicated that Plaintiff's private information was among the information accessed or acquired during the Data Breach.

74. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts for unusual activity. This time has been lost forever and cannot be recaptured. This time was spent at Defendant's direction. In particular, Defendant indicated in its Notice of Data Breach that Plaintiff should spend time to protect her identity in order to mitigate her losses.

75. Plaintiff is very careful about sharing her sensitive PII, PHI, and PBI. She has never knowingly transmitted unencrypted sensitive PII, PHI, and PBI over the internet or any other unsecured source.

76. Plaintiff stores any documents containing her sensitive PII, PHI, and PBI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

77. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII, PHI, and PBI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff suffered lost time,

annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

78. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, PHI, and PBI being placed in the hands of unauthorized third parties and possibly criminals.

79. Plaintiff has a continuing interest in ensuring that her PII, PHI, and PBI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

80. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

81. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> All United States residents whose PII, PHI, and/or PBI was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around April 22, 2022 (the "Nationwide Class").

82. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

> All Illinois residents whose PII, PHI, and/or PBI was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around April 22, 2022 (the "Illinois Class").

83. In addition to the Nationwide and Illinois Classes, Plaintiff asserts claims on behalf of a separate subclass defined as follows:

> All United States residents whose PBI was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data

Breach that Defendant sent to Plaintiff and other Class Members on or around April 22, 2022 (the "PBI Class").

84. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

85. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

86. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide, Illinois, and PBI class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds, if not thousands, of individuals whose PII, PHI and/or PBI may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

87. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII, PHI, and PBI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII, PHI, and PBI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII, PHI, and PBI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII, PHI, and PBI of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII, PHI, and PBI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII, PHI, and PBI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII, PHI, and PBI of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Defendant unlawfully disclosed and/or disseminated Plaintiff's and Class Members' PBI in violation of ILCS 740 14/15(d)(1)-(4);

n. Whether Defendant failed to protect Plaintiff's and Class Members' PBI in violation of ILCS 740 14/15(e);

o. Whether Defendant was negligent, intentional, or reckless in unlawfully disclosing and/or failing to protect Plaintiff's and Class Members' PBI;

p. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

q. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

88. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII, PHI, and PBI compromised as a result of the Data Breach, due to Defendant's misfeasance.

89. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

90. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

91. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

92. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

93. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

94. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

95. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII, PHI, and PBI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

96. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

97. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII, PHI, and PBI;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII, PHI, and PBI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII, PHI, and PBI had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII, PHI, and PBI of Plaintiff and Class Members;

i. Whether Defendant unlawfully disclosed and/or failed to protect Plaintiff's and Class Members' PBI in violation of ILCS 740 14/15; and

j. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

98. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

99. Plaintiff and the Class entrusted Defendant with their PII, PHI, and PBI.

100. Plaintiff and the Class entrusted their PII, PHI, and PBI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and/or

PHI for business purposes only, and/or not disclose their PII, PHI, and PBI to unauthorized third parties.

101. Defendant has full knowledge of the sensitivity of the PII, PHI, and PBI and the types of harm that Plaintiff and the Class could and would suffer if the PII, PHI, and PBI were wrongfully disclosed.

102. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII, PHI, and PBI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

103. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII, PHI, and PBI of Plaintiff and the Classes in Defendant's possession was adequately secured and protected.

104. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and/or PHI they were no longer required to retain pursuant to regulations.

105. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII, PHI, and PBI of Plaintiff and the Class.

106. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, PHI, and PBI, a necessary part of obtaining services from Defendant.

107. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

108. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

109. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII, PHI, and PBI of Plaintiff and the Class, the critical importance of providing adequate security of that PII, PHI, and PBI, and the necessity for encrypting PII, PHI, and PBI stored on Defendant's systems.

110. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII, PHI, and PBI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

111. Plaintiff and the Class had no ability to protect their PII, PHI, and PBI that was in, and possibly remains in, Defendant's possession.

112. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

113. Defendant had and continue to have a duty to adequately disclose that the PII, PHI, and PBI of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such

notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII, PHI, and PBI by third parties.

114. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII, PHI, and PBI of Plaintiff and the Class.

115. Defendant has admitted that the PII, PHI, and PBI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

116. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII, PHI, and PBI of Plaintiff and the Class during the time the PII, PHI, and PBI was within Defendant's possession or control.

117. Defendant improperly and inadequately safeguarded the PII, PHI, and PBI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

118. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII, PHI, and PBI of Plaintiff and the Class in the face of increased risk of theft.

119. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII, PHI, and PBI.

120. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII, PHI, and PBI they were no longer required to retain pursuant to regulations.

121. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

122. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII, PHI, and PBI of Plaintiff and the Class would not have been compromised.

123. There is a close causal connection between Defendant's failure to implement security measures to protect the PII, PHI, and PBI of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII, PHI, and PBI of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII, PHI, and PBI by adopting, implementing, and maintaining appropriate security measures.

124. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII, PHI, and PBI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

125. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII, PHI, and PBI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII, PHI, and PBI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

126. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

127. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

128. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

129. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII, PHI, and PBI is used; (iii) the compromise, publication, and/or theft of their PII, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, PHI, and PBI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII, PHI, and PBI of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

130. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

131. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII, PHI, and PBI in its continued possession.

132. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

133. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

134. Plaintiff and the Class entrusted their PII, PHI, and PBI to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

135. In their Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII, PHI, or PBI.

136. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

137. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

138. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

139. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

140. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

141. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII, PHI, and PBI.

142. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff' and Class Members' PII, PHI, and PBI.

143. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

144. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

145. Defendant acquired the monetary benefit and PII, PHI, and PBI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

146. If Plaintiff and Class Members knew that Defendant had not secured their PII, PHI, and PBI, they would not have agreed to provide their PII, PHI, and PBI to Defendant.

147. Plaintiff and Class Members have no adequate remedy at law.

148. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, PHI, and PBI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not

limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII, PHI, and PBI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

149. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

150. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT IV
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On behalf of Plaintiff and the Illinois Class)

151. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

152. Plaintiff and the Illinois Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Illinois Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

153. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

154. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Illinois Class's sensitive PII, PHI, and PBI from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff and the Illinois Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII, PHI, and PBI of Plaintiff and the Illinois Class; (3) failing to disclose or omitting materials facts to Plaintiff and the Illinois Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII, PHI, and PBI of Plaintiff and the Illinois Class; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff and the Illinois Class's PII, PHI, and PBI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

155. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Illinois Class and defeat their reasonable expectations about the security of their PII, PHI, and PBI.

156. Defendant intended that Plaintiff and the Illinois Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

157. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Class. Plaintiff and the Illinois Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

158. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Illinois Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

159. As a result of Defendant's wrongful conduct, Plaintiff and the Illinois Class were injured in that they never would have provided their PII, PHI, and PBI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII, PHI, and PBI from being hacked and taken and misused by others.

160. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Illinois Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, PHI, and PBI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII, PHI, and PBI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI

compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

161. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT V
Violation of 740 ILCS 14/, *et seq*.
(On behalf of Plaintiff and the PBI Class)

162. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

163. Defendant is a "private entity" as defined by BIPA. *See* ILCS 740 14/1.

164. BIPA is an informed consent statute that achieves its goal by making it unlawful for a company to disclose information unless *first*: "(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." ILCS 740 14/15(d)(1)-(4).

165. BIPA also requires the following: "[a] private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers, and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the

manner in which the private entity stores, transmits, and protects other confidential and sensitive information." ILCS 740 14/15(d)(1)-(4).

166. Defendant violated ILCS 740 14/15(d)(1)-(4) because it disclosed Plaintiff's and Class Members' PBI without authorization or under the approved exceptions.

167. Defendant violated ILCS 740 14/15(e) because it failed to protect Plaintiff's and Class Members' PBI.

168. Defendant acted negligently in violating ILCS 740 14/15.

169. Defendant acted recklessly in violating ILCS 740 14/15.

170. Defendant acted intentionally in violating ILCS 740 14/15.

171. As a direct and proximate result of Defendant's violations of the BIPA, upon information and belief, Plaintiff and the Illinois Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII, PHI, and PBI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, PHI, and PBI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, PHI, and PBI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII, PHI, and PBI in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII, PHI, and PBI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.,

172. Pursuant to 740 ILCS 14/1, *et seq*., Plaintiff on behalf of herself and Class Members seeks the following: (i) injunctive and equitable relief as necessary to protect the interests of the Plaintiff and Class by requiring Defendant to comply with BIPA's requirements for unlawful disclosure and duty to protect BIPA; (ii) injunctive and equitable relief as necessary to protect the public good and the public's right to issuance of a written policy to ensure that Defendant complies with the written policy; (iii) statutory damages of $1,000 per violation for each of Defendant's negligent violations of BIPA pursuant to 740 ILCS 14/20(1) or $5,000 for Defendant's intentional, or reckless violation of BIPA pursuant to 740 ILCS 14/20(2); and (iv) reasonably attorneys' fees and costs and expenses pursuant to 740 ILCS 14/20(3).

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the Illinois Class, and the BIPA Class, and appointing Plaintiff and her Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII, PHI, and PBI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII, PHI, and PBI of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII, PHI, and PBI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised,

hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the

threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of statutory damages of $1,000 for each of Defendant's violation of BIPA, pursuant to 740 ILCS 14/20(1) and/or $5,000 for each of Defendant's violations of BIPA, pursuant to 740 ILCS 14/20(2);

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: May 13, 2022

Respectfully Submitted,

/s/ Gary M. Klinger

Gary M. Klinger (IL Bar No. 6303726)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Bryan L. Bleichner*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

**Pro Hac Vice Application forthcoming*

Counsel for Plaintiff and Putative Class